Drayton Bassett Parish Council

Parish Clerk: Robert Pritchard
Email: parishclerk@draytonbassett-pc.gov.uk

January 2026

REPORT OF THE CLERK

Staffordshire Playing Fields Association:

The membership form has been submitted and membership fee paid. The SPFA have confirmed receipt of payment.

Banking:

The new Unity Banking Trust bank account has been opened, and the switching service has completed. All funds and direct debits have been transferred over.

Dog poo bags:

A replacement key has been sourced for the bag dispenser on Heathley Lane and it has been refilled with bags.

Playing Fields:

A CIL bid has been submitted to Lichfield District Council for £75,000 to improve the BMX track and install new sporting equipment on the playing fields.

LDC Clean & Green bid:

The council has secured funding from Lichfield District Council to cover the costs of the new dog poo bin and bag dispenser on the playing fields. A duel bin and bag dispenser will be sourced and contractor commissioned to install it.

Payroll Provider:

The new provider has been engaged and will take over payroll functions from January 2026.

Interim Internal Audit:

The interim internal audit was undertaken in December, no compliance issues have been identified.

Speed Indicator Device (SID)

A location was agreed with Staffordshire County Council (SCC) to install the SID, however before permission was granted, SCC have stopped all permissions pending a policy review. We have no indication on the timescales or outcome of this review. Lichfield District Council has been informed.

Public Space Protection Order (Dogs on leads):

Lichfield District Council has since confirmed that it will not implement any PSPO for the playing fields. The proposal was refused by the Regulatory and Licensing Committee at Lichfield District Council.

Drayton Bassett Parish Council **Reconciliation Report – November 2025**

Opening Balance 1/11/25	**46,056.57**
Income for the period	-
Expenditure for the period	2,059.14
Closing Balance 30/11/25	**43,997.43**

Breakdown of payments:

					NET		VAT		GROSS	CREDIT
03/11/2025	Pennon Water Services	DD	Utilities	£	46.09	£	-	£	46.09	
03/11/2025	Lichfield Council	DD	Rates	£	175.00	£	-	£	175.00	
05/11/2025	R Pritchard (Currys PC World)	FPR	IT	£	279.98	£	56.00	£	335.98	
18/11/2025	Sage	DD	Payroll	£	11.00	£	2.20	£	13.20	
18/11/2025	SLCC	FPO	Training	£	45.00	£	9.00	£	54.00	
18/11/2025	Lauren Hodge	FPO	Grounds Maintainance	£	1,050.00	£	-	£	1,050.00	
18/11/2025	Robert Pritrchard	FPO	Salaries	£	287.90	£	-	£	287.90	
18/11/2025	Robert Pritchard	FPO	Stationary	£	8.00	£	-	£	8.00	
19/11/2025	ICO	DD	ICO Fee	£	47.00	£	-	£	47.00	
21/11/2025	EDF	BP	Utilities	£	32.15	£	1.61	£	33.76	
27/10/2025	Water Plus	DD	Water	£	8.21	£	-	£	8.21	
			Total expenditure	**£**	**1,990.33**	**£**	**68.81**	**£**	**2,059.14**	**£ -**

Bank balance agreed to bank statement

Signed by Chairman _____

Date _____

Drayton Bassett Parish Council **Reconciliation Report – December 2025**

Opening Balance 1/12/25	**43,997.43**
Income for the period	-
Expenditure for the period	969.23
Closing Balance 30/12/25	**43,028.20**

Breakdown of payments:

				NET	VAT	GROSS	CREDIT
03/12/2025	Lloyds Bank	PAY	Bank Charges	£ 4.25	£ -	£ 4.25	
03/12/2025	Lichfield Council	DD	Rates	£ 175.00	£ -	£ 175.00	
07/12/2025	R Bridge	FPO	Handyman	£ 291.66		£ 291.66	
18/12/2025	Sage	DD	Payroll	£ 11.00	£ 2.20	£ 13.20	
17/12/2025	SLCC	FPO	SLCC Membership Fee	£ 57.78		£ 57.78	
17/12/2025	JRB Enterprise Ltd	FPO	Waste bags	£ 58.80	£ 11.76	£ 70.56	
17/12/2025	Robert Pritrchard	FPO	Salaries	£ 287.90	£ -	£ 287.90	
17/12/2025	Staffordshire Playing Fields Assoc	FPO	Membership Fee	£ 20.00	£ -	£ 20.00	
29/12/2025	Lloyds Bank	PAY	Bank Charges	£ 4.25	£ -	£ 4.25	
23/12/2025	EDF	BP	Utilities	£ 34.69	£ 1.73	£ 36.42	
27/10/2025	Water Plus	DD	Water	£ 8.21	£ -	£ 8.21	
			Total expenditure	**£ 953.54**	**£ 15.69**	**£ 969.23**	**£ -**

Bank balance agreed to bank statement

Signed by Chairman _____

Date _____

Drayton Bassett Parish Council

IT Policy

Introduction

Each council will have its own IT setup and, as such, a single ‘one-size-fits-all’ IT policy is unlikely to be appropriate. Some smaller parish councils may operate with minimal equipment, while others may manage multiple devices connected to a central server. These guidelines are intended to help councils identify key considerations when developing or updating their own IT policy.

Councils that use external IT providers should ensure their policies accurately reflect current practices and contractual arrangements.

Purpose of the IT Policy

The purpose of an IT policy is to establish clear parameters for how councillors, staff, and other authorised users use council-provided technology or equipment in the course of their duties. A well-defined policy helps to:

- Set expectations for appropriate use of equipment and systems;
- Raise awareness of risks associated with IT use;
- Safeguard the council’s data and digital assets;
- Clarify what constitutes acceptable and unacceptable use;
- Outline the consequences of policy breaches.

Councils will also need to determine and clearly state whether limited personal use of IT equipment is permitted (for example, checking personal email or online shopping during lunch breaks).

Monitoring of IT Use

As an IT provider, the council has the right to monitor the use of its IT equipment and systems, provided there is a legitimate reason for doing so and councillors, employees and other authorised users are informed that such monitoring may take place. Any monitoring must be proportionate and comply with relevant data protection and privacy laws. Other persons may be included if they access or use council systems e.g. if they have a council e-mail address

Scope of this policy

This policy applies to all councillors, staff, and other authorised users, regardless of their working location or pattern, including those who are home-based, office-based, or work on a flexible or part-time basis. It sets out the expectations for the appropriate use of IT equipment and systems provided by the council.

Computer use

1.1 Hardware

1.1.1 Council computer equipment is provided to staff for council purposes; however reasonable personal use is permitted. Any personal use of our computers and systems should not interrupt our daily council work in any way. Councillors, staff, and other authorised users are asked to restrict any personal use to official lunch breaks or before or after working hours.

1.1.2 Users will lock computers when leaving unattended to prevent unauthorised access. This applies to all council and personal devices used for work. Failure to comply may lead to disciplinary action.

1.1.3 All computer and other electronic equipment supplied should be treated with good care at all times. Computer equipment is expensive, and any damage sustained to any equipment will have a financial impact on the council.

1.1.4 Computer and electronic hardware should be kept clean, and every precaution taken to prevent food and drink being dropped or spilled onto it.

1.1.5 All computer and mobile equipment will carry a number which is logged against the current owner of that equipment. A database of equipment issued will be kept.

1.1.6 Equipment should not be dismantled or reassembled without seeking advice.

1.1.7 Councillors, staff, and other authorised are not to purchase any computer or mobile equipment (including software). Unless previously authorised by the clerk or council.

Equipment

2.1 Portable equipment

2.1.1 Portable equipment includes laptop computers, netbooks, tablets, mobile and smart phones with email capability and access to the internet etc.

2.1.2 It is particularly emphasised that council back-up procedures specific to portable equipment should be followed at all times.

2.1.3 All portable computers must be stored safely and securely when not in use in the office, i.e. when travelling or when working from home. Portable equipment (unless locked in a secure cabinet or office) should be kept with or near the user at all times; should not be left unattended when away from council premises and should never be left in parked vehicles or at any council or non-council premises.

2.1.4 It is important to ensure all portable devices are protected with encryption in case they are lost or stolen. All smartphones or tablets that hold council data, including emails and files, must be protected with a pin code. Where possible, these devices should also be programmed to erase all content after several unsuccessful attempts to break in. Any security set on these devices must not be disenabled or removed.

2.1.5 Multi-Factor Authentication (MFA) is a security process that requires users to verify their identity using two or more independent methods—for example, entering a password (something you know) and confirming a code sent to your mobile device (something you have). This significantly reduces the risk of unauthorised access to systems and sensitive data. NALC recommends implementing MFA as a best practice to enhance information security and support compliance with data protection obligations under the UK GDPR and the Data Protection Act 2018.

2.1.6 If an item of portable equipment is lost or damaged this should be reported to the Clerk or council as appropriate.

2.1.7 Under no circumstances should any non public meeting or conversation be recorded without the permission of those present. This does not affect statutory rights (under The Openness of Local Government Regulations 2014).

2.1.8 In addition, the council does not permit webcams (which may be pre-installed on many laptops) to be used in the workplace, other than for conference calls for council purposes.

2.2 Use of own devices

2.2.1 The Council recognises that some councillors, staff, and other authorised users may wish to use their own smartphones, tablets, laptops etc to access our servers, private clouds or networks for normal council purposes, including, but not limited to, reading their emails, accessing documents stored on the council's cloud storage. Any such use of personal devices will be at the discretion of the council, but consent for standard systems (MS Windows, Mac OS X, Linux - in commercial configurations) will normally be permitted. Such devices should be kept up to date so that any vulnerabilities in the operating system or other software on the device are appropriately patched or updated.

2.2.2 However, the same security precautions apply to personal devices as to the council's desktop equipment.

2.2.3 Councillors, staff, and other authorised persons that use council systems are expected to use all devices in an ethical and respectful manner and in accordance with this policy.

2.2.4 In cases of legal proceedings against the council or to comply with legal requests, the council may need to temporarily take possession of a device, whether council-owned or personal to retrieve the relevant data.

2.2.5 Wherever possible the user should maintain a clear separation between the personal data processed on the council's behalf and that processed for their own personal use, for example, by using different apps for council and personal use. If the device supports both work and personal profiles, the work profile must always be used for work-related purposes.

2.2.6 Councillors, staff, and other authorised users who intend to use their own devices via the council's infrastructure must ensure that they:

- use a strong password or PIN to protect their device(s) from being accessed. For smartphones and tablets this should lock the device after [specify number] of failed login attempts;
- configure their device(s) to automatically prompt for a password after a period of inactivity;
- always password protect any documents containing confidential information that are sent as attachments to an email, and notify the password separately (preferably by a means other than email);
- for smartphones and tablets, activate the automatic device wipe function (where available). Note that use of the remote wipe function may also involve the removal of the individual's personal data. Councillors, staff, and other authorised users are therefore advised to keep personal data separate from council data where possible;
- ensure secure WiFi networks are used;
- ensure that work-related data cannot be viewed or retrieved by family or friends who may use the device;
- inform the council or the clerk if their device(s) is/are lost, stolen, or inappropriately accessed where there is risk of access to council data or resources. To prevent phones being used, they will need to retain the details of their IMEI number and the SIM number of the device as their provider will require this to deactivate it.

2.2.7 Personal data relating to councillors, staff, and other authorised users, associates, residents, external stakeholders should not be saved to any personal accounts with third-party storage cloud service providers as this may breach data protection legislation or create a security risk if the device is lost or stolen. This applies especially if the passwords used to store/access data are saved onto the device, or if the service permits councillors, staff, and other authorised users to remain logged in between sessions.

2.2.8 Personal information and sensitive data should never be saved on councillors, staff, or other authorised users own devices as this may breach confidentiality agreements, especially if the device is used by other people from time to time. The following data must never be accessed or processed on a personal device.

2.2.9 If removable media are used to transfer data (e.g. USB drives or CDs), the user must also securely delete the data on the media once the transfer is complete.

2.2.10 Any council work done on user's own equipment should be stored securely and password protected and should always be backed up in accordance with the council's standard backup procedures.

2.2.11 If transferring data, either by email or by other means, this should be done through an encrypted channel, such as a virtual private network (VPN) or a secure web protocol (https://). Unsecured wireless networks should not be used.

2.2.12 Prior to the disposal of any device that has work data stored on it, and in the event of a user leaving the council, councillors, staff, and other authorised users are required to allow a council chosen IT provider access to the device to ensure that all passwords, user access shortcuts and any identifiable data are removed from the device.

2.2.13 Councillors, staff, and other authorised users must take responsibility for understanding how their device(s) work in respect to the above rules if they are accessing council servers/services via their own IT equipment. Risks to the user's personal device(s) include data loss as a result of a crash of the operating system, bugs and viruses, software or hardware failures and programming errors rendering a device inoperable. The council will use reasonable endeavours to assist, but councillors, staff, and other authorised users are personally liable for their own device(s) and for any costs incurred as a result of the above.

Health and safety

3.1.1 Councillors, staff, and other authorised users who work in council offices will be provided with an appropriate workstation.

3.1.2 The council has a duty to ensure that regular appropriate eye tests, carried out by a competent person, are offered to employees using display screen equipment.

3.1.3 Any VDU user who feels that their workstation requires changes to make it compliant must speak to the clerk.

If any hazards are detected at a workstation, including ‘noises’ from the IT equipment, this should be reported immediately to the clerk.

Password and Authentication Policy

4.1.1 All user accounts must be protected by strong, secure passwords. The council follows the National Cyber Security Centre (NCSC) recommendations for creating passwords using three random words (e.g. PurpleCandleRiver). This method helps create passwords that are both strong and easy to remember, while offering effective protection against common cyber threats such as brute-force attacks. This approach is endorsed in NALC guidance.

In addition to strong passwords, Multi-Factor Authentication (MFA) should be enabled wherever possible. MFA requires users to provide two or more independent forms of verification—for example, a password (something you know) and a code sent to your phone (something you have). This significantly reduces the risk of unauthorised access to systems and personal data.

To further strengthen account security:

- Initial user account passwords must be generated by the IT provider.
- Default passwords provided by vendors or the IT provider must be changed immediately upon installation or setup.
- Service or System (e.g. Website) account passwords are generated and managed by the IT provider.

- The council recommends these practices as part of its commitment to robust information security and to support compliance with the UK GDPR and the Data Protection Act 2018.

For more guidance, see the NCSC's advice on password security: NCSC Password Guidance

4.1.2 Access to Passwords

- Passwords are personal and must not be shared under any circumstances.
- Only the assigned user of an account may access or use the associated password.
- In exceptional cases (e.g., incident response or employee offboarding), access to system credentials may be granted to authorised personnel from the IT provider with appropriate approvals and logging.
- Administrative credentials must be stored securely and only accessible to authorised personnel with a copy provided to the chairman of council, in a sealed envelope, only to be accessed in an emergency.

4.1.3 Password Storage and Management

- Passwords must not be stored in plain text or written down in insecure locations.
- Passwords must be stored using a council-approved, encrypted password manager (e.g., LastPass, Bitwarden, or KeePass).

4.1.4 Password Change Requirements

- Immediately change password if compromise is suspected.

4.1.5 Password Access Control and Logging

- All access to administrative or shared credentials must be logged and auditable.
- Attempts to access unauthorized passwords will be treated as a security incident.

4.1.6 Responsibility

- Users are responsible for creating and maintaining secure passwords for their accounts.

Monitoring

5.1.1 The council reserves the right to monitor and maintain logs of computer usage and inspect any files stored on its network, servers, computers, or associated technology to ensure compliance with this policy as well as relevant legislation. Internet, email, and computer usage is continually monitored as part of the council's protection against computer viruses, ongoing maintenance of the system, and when investigating faults.

5.1.5 The council will monitor the use of electronic communications and use of the internet in line with the Investigatory Powers (Interception by Councils etc for Monitoring and Record-keeping Purposes) Regulations 2018.

5.1.6 Monitoring of an employee's email and/or internet use will be conducted in accordance with an impact assessment that the council has carried out to ensure that monitoring is necessary and proportionate. Monitoring is in the council's legitimate interests and is to ensure that this policy is being complied with.

5.1.7 The information obtained through monitoring may be shared internally, including with relevant councillors and IT staff if access to the data is necessary for performance of their roles. The information may also be shared with external HR or legal advisers for the purposes of seeking professional advice. Any external advisers will have appropriate data protection policies and protocols in place.

5.1.8 The information gathered through monitoring will be retained only long enough for any breach of this policy to come to light and for any investigation to be conducted.

5.1.9 Councillors, staff, and other authorised users have a number of rights in relation to their data, including the right to make a subject access request and the right to have data rectified or erased in some circumstances. You can find further details of these rights and how to exercise them in the council's data protection policy.

5.1.10 Such monitoring and the retrieval of the content of any messages may be for the purposes of checking whether the use of the system is legitimate, to find lost messages or to retrieve messages lost due to computer failure, to assist in the investigation of wrongful acts, or to comply with any legal obligation.

5.1.11 The council reserves the right to inspect all files stored on its computer systems in order to assure compliance with this policy. The council also reserves the right to monitor the types of sites being accessed and the extent and frequency of use of the internet at any time, both inside and outside of working hours to ensure that the system is not being abused and to protect the council from potential damage or disrepute.

5.1.12 Any use that the council considers to be 'improper', either in terms of the content or the amount of time spent on this, may result in disciplinary proceedings.

5.1.13 All computers will be periodically checked and scanned for unauthorised programmes and viruses.

Remote working

6.1.1 Increased IT security measures apply to those who work away from their normal place of work (e.g. whilst travelling, working from home, as follows:

- if logging into the council's systems or services remotely, using computers that either do not belong to the council or are not owned by the user, any passwords must not be saved, and the user must log out at the end of the session deleting all logs and history records within the browser used. If the configuration of the devise does not clearly support these actions (for example at an internet café), council services should not be accessed from that device;

- the location and direction of the screen should be checked to ensure confidential information is out of view. Steps should be taken to avoid messages being read by other people, including other travellers on public transport etc;
- any data printed should be collected and stored securely;
- all electronic files should be password protected and the data saved to the council's system/services when accessible;
- papers, files or computer equipment must not be left unattended at a premises unless arrangements have been made with a responsible person at the premises for them to be kept in a locked room or cabinet if they are to be left unattended at any time;
- any data should be kept safely and should only be disposed of securely;
- papers, files, data sticks/storage, flash drive or backup hard drives should not be left unattended in cars, except where it is entirely unavoidable for short periods, in which case they must be locked in the boot of the car. If staying away overnight, council data should be taken into the accommodation, care being taken that it will not be interfered with by others or inadvertently destroyed;
- where possible the ability to remotely wipe any mobile devices that process sensitive information should be retained in the case of loss or theft;
- Councillors, staff, and other authorised users who work away from the office with sensitive data should be equipped with a screen privacy filter for mobile devices and should use this at all times when accessing such data away from the office.

6.1.2 Similarly, use of paid for Wi-Fi access, for example at airports should be carefully monitored and restricted to essential council use.

Email

7.1.1 Council email facilities are intended to promote effective and speedy communication on work-related matters. Although we encourage the use of email, it can be risky. Councillors, staff, and other authorised users need to be careful not to introduce viruses onto council systems and should take proper account of the security advice below.

7.1.2 On occasion, it will be quicker to action an issue by telephone or face to face, rather than via protracted email chains. Emails should not be used as a substitute for face to face or telephone conversations. Councillors, staff, and other authorised users are expected to decide which is the optimum channel of communication to complete their tasks quickly and effectively.

7.1.3 These rules are designed to minimise the legal risks run when using email at work and to guide councillors, staff, and other authorised users as to what may and may not be done. If there is something which is not covered in the policy, councillors, staff, and other authorised users should ask the Clerk rather than assuming they know the right answer.

7.1.4 All councillors, staff, and other authorised users who need to use email as part of their role will normally be given their own council email address and account. The council may, at any time, withdraw email access, should it feel that this is no longer necessary for the role or that the system is being abused.

7.1.5 Email messages sent on the council's account are for council use only. Personal use is not permitted.

Use of the Internet

8.1 Copyright

8.1.1 Much of what appears on the Internet is protected by copyright. Any copying without permission, including electronic copying, is illegal and therefore prohibited. The Copyright, Designs and Patents Act 1988 set out the rules. The copyright laws not only apply to documents but also to software. The infringement of the copyright of another person or organisation could lead to legal action being taken against the council and damages being awarded, as well as disciplinary action, including dismissal, being taken against the perpetrator.

8.1.2 It is easy to copy electronically, but this does not make it any less an offence. The council's policy is to comply with copyright laws, and not to bend the rules in any way.

8.1.3 Councillors, staff, and other authorised users should not assume that because a document or file is on the Internet, it can be freely copied. There is a difference between information in the 'public domain' (which is no longer confidential or secret information but is still copyright protected) and information which is not protected by copyright (such as where the author has been dead for more than 70 years).

8.1.4 Usually, a website will contain copyright conditions; these warnings should be read before downloading or copying.

8.1.5 Copyright and database right law can be complicated. Councillors, staff, and other authorised users should check with the clerk if unsure about anything.

8.2 Trademarks, links and data protection

8.2.1 The council does not permit the registration of any new domain names or trademarks relating to the council's names or products anywhere in the world, unless authorised to do so. Nor should they add links from any of the council's web pages to any other external sites without checking first with the clerk.

8.2.2 Special rules apply to the processing of personal and sensitive personal data. For further guidance on this, see the council's data protection policy, a copy of which is on the council website.

8.3 Accuracy of information

8.3.1 One of the main benefits of the internet is the access it gives to large amounts of information, which is often more up to date than traditional sources such as libraries. Be aware that, as the internet is uncontrolled, much of the information may be less accurate than it appears.

Use of social media

9.1.1 Social media includes blogs; Wikipedia and other similar sites where text can be posted; multimedia or user generated media sites (YouTube); social networking sites (such as Facebook, LinkedIn, X (formerly known as Twitter), Instagram, TikTok, etc.); virtual worlds (Second Life); text messaging and mobile device communications and more traditional forms of media such as TV and newspapers. Care should be taken when using social media at any time, either using council systems or at home.

9.1.2 The council recognises the importance of councillors, staff, and other authorised users joining in and helping to shape sector conversation and enhancing its image through blogging and interaction in social media. Therefore, where it is relevant to use social networking sites as part of the individual's position, this is acceptable.

However, inappropriate comments and postings can adversely affect the reputation of the council, even if it is not directly referenced. If comments or photographs could reasonably be interpreted as being associated with the council, or if remarks about external stakeholders could be regarded as abusive, humiliating, sexual harassment, discriminatory or derogatory, or could constitute bullying or harassment, the council will treat this as a serious disciplinary offence. Councillors, staff, and other authorised users should be aware that parishioners or other local organisations may read councillors, staff, and other authorised users' personal weblogs, to acquire information, for example, about their work, internal council business, and employee morale. Therefore, even if the council is not named, care should be taken with any views expressed.

9.1.3 To protect both the council and its interests, everyone is required to comply with the following rules about social media, whether in relation to their council role or personal social networking sites, and irrespective of whether this is during or after working hours:

- Contacts from any of the council's databases should not be downloaded and connected with on LinkedIn or other social networking sites with electronic address book facilities, unless this has been authorised.
- Any blog that mentions the council, its current work, councillors, employees, other users associated with the council, partner organisations, local groups, suppliers, parishioners, should identify the author as one of its councillors or employees and state that the views expressed on the blog or website are theirs alone and do not represent the views of the council. Even if the council is not mentioned, care should be taken with any views expressed on social media sites and any views should clearly be stated to be the writer's own (e.g. via a disclaimer statement such as: "The comments and other content on this site are my own and do not represent the positions or opinions of my employer/ the council.") Writers must not claim or give the impression that they are speaking on behalf of the council.
- Any employee who is developing a site or writing a blog that will mention the council,
- The council expects councillors, staff, and other authorised users to be respectful about the council and not to engage in any name calling or any behaviour that will reflect negatively on its reputation. Any unauthorised use of copyright materials, any unfounded or derogatory statements, or any misrepresentation is not viewed favourably and could constitute gross misconduct.
- Photos or videos that include employees or other workers wearing uniforms or clothing displaying the council's name or logo should not be posted on social media if

they could reflect negatively on the individual, their role, their colleagues, or the council. Additionally, photos, videos, or audio recordings must not be taken on council premises without explicit permission

- Comments posted by councillors, staff, and other authorised users on any sites should be knowledgeable, accurate and professional and should not compromise the council in any way.
- Inappropriate conversations with should not take place on any social networking sites, including forums.
- Any writing about or displaying photos or videos of internal activities that involves current councillors, staff, and other authorised persons, might be considered a breach of data protection and a breach of privacy and confidentiality. Therefore, their permission should be gained prior to uploading any such material. Details of any kind relating to any events, conversations, materials or documents that are meant to be private, confidential or internal to the council should not be posted. This may include manuals; procedures; training documents; non-public financial or operational information; personal information regarding other councillors, staff, and other authorised users anything to do with a disciplinary case, grievance, allegation of bullying/harassment or discrimination, or legal issue; any other secret, confidential, or proprietary information or information that is subject to confidentiality agreements. This does not affect statutory requirements to publish information including under the Freedom of Information Act.
- Councillors, staff, and other authorised users must be aware that they are personally liable for anything that they write or present online (including on an online forum or blog, post, feed or website). Councillors should always be mindful of the Members Code of Conduct and Nolan Principles. Employees may be subject to disciplinary action for comments, content, or images that are defamatory, embarrassing, pornographic, proprietary, harassing, libellous, or that can create a hostile work environment. They may also be sued by other organisations, and any individual or council that views their comments, content, or images as defamatory, pornographic, proprietary, harassing, libellous or creating a hostile work environment. In addition, other councillors, staff, and other authorised users can raise grievances for alleged bullying and/or harassment.
- Postings to websites or anywhere on the internet and social media of any kind, or in any press or media of any kind, should not breach copyright or other law or disclose confidential information, defame or make derogatory comments about the council or disclose personal data or information about any individual that could breach data protection legislation.
- Contacts by the media relating to the council, should be referred to the Clerk for advice.
- Councillors, staff, and other authorised users who use sites such as LinkedIn and Facebook must ensure that the information on their profile is accurate and up to date and must update their profile on leaving the council.
- Councillors, staff, and other authorised users who use X.com, LinkedIn, or other social media/networking sites for council development purposes must ensure they provide the council with login details, including password(s), so that these sites can be accessed and updated in their absence.
- Councillors, staff, and other authorised users who have left the council must not post any inappropriate comments about the council or its councillors, staff, and other

authorised users on LinkedIn, Facebook, X.com or any other social media/networking sites.

- During your employment/ involvement with the council, you may create or obtain access to a variety of professional contacts and confidential information. This includes, but is not limited to, contacts made through professional networking platforms such as LinkedIn, where those contacts have been established or maintained in your capacity as a councillor, member of staff, or other authorised user. All such contacts will be considered council property and may be subject to disclosure upon request.

9.1.4 Note that the council may, from time to time, monitor external postings on social media sites. Any employee who has a profile (for example on LinkedIn or Facebook) must not misrepresent themselves or their role with the council. Councillors, staff, and other authorised users are also advised that social media sites are not an appropriate place to air council concerns or complaints: these should be raised with the council or formally through the grievance procedure.

9.1.5 It is important to note that external stakeholders contact details and information remain the property of the council. In addition, councillors, staff, and other authorised users leaving the council will be required to delete all council-related data, including external stakeholders contact details, from any personal device/equipment.

Misuse

Misuse of IT systems and equipment is not in line with the council's standards of conduct and will be taken seriously. Any inappropriate or unauthorised use may lead to formal action, including disciplinary proceedings or, in serious cases, dismissal.

Policy	Review Required	Adopted	Last Reviewed	Next Review due	Legal Reference
Anti Harassment Policy and Procedure	Biannual	Yes	May-25	2027	Equality Act 2010
Biodiversity Policy	Biannual	Yes	Sep-25	2027	Natural Environment and Rural Communities Act 2006
Code of Conduct	Biannual	Yes	Jan-23	2027	Localism Act 2011 S27(2)
Civility and Respect Pledge	Biannual	Yes	Nov-25	2026	Equality Act 2010
Complaints Policy and Procedure	Biannual	Yes	Nov-24	2026	
Contractors Policy	Biannual	Yes	Jul-23	2026	Procurement Act 2023
Data Privacy and Protection Policy	Biannual	Yes	Mar-23	2026	General Data Protection Regulation (GDPR) 2016 / Data Protection Act (DPA) 2018.
Data Protection and Your Rights Policy	Biannual	Yes	Nov-24	2026	General Data Protection Regulation (GDPR) 2016 / Data Protection Act (DPA) 2018.
Dignity at Work Policy	Biannual	Yes	Nov-25	2027	Equality Act 2010 (Part 5)
Equality and Diversity Policy	Biannual	Yes	Nov-25	2027	Equality Act 2010
Financial Regulations	Annual	Yes	May-25	May 2026	Accounts and Audit Regulations 2015 / Local Government Act 1972 (various) / Local Audit and Accountability Act 2014
Grant Awarding Policy	Biannual	Yes	Feb-24	2026	
Grievance procedure for Employees	Biannual	Yes	May-22	2026	Employment Rights Act 1996 / Equality Act 2010
Memorial Benches and Trees Policy	Biannual	Yes	Jun-25	2027	Highways Act 1980 / Equaliaty Act 2010
Publication Scheme	Biannual	Yes	May-25	As required	The Freedom of Information Act / Transparency code for smaller authorities
Risk Register	Biannual	Yes	May-25	As required	Proper Practices
Retention of Documents and Records	Biannual	Yes	May-25	2027	Freedom of Information Act 2000
Social Media Policy	Biannual	Yes	Oct-23	2026	
Councillor and Staff Training Policy	Biannual	Yes	Sep-25	2027	Equality Act 2010 / Localism Act 2010
Standing Orders	Annual	Yes	May-25	May 2026	Local Government Act 1972 (various)
Tree Policy	Biannual	Yes	Jan-24	2026	Health and Safety
Health and Safety Policy	Biannual	Yes	May-22	2026	Health and Safety at Work Act 1974
IT Policy	Biannual	No / Draft	N/A	Jan/Feb 2026	Assertion 10 / Data Protection Act / GDPR

Local Council Award Scheme Application Form

COUNCIL NAME	Drayton Bassett Parish Council
DATE OF APPLICATION	20/01/26
AWARD LEVEL	Bronze Level

Please read through the scheme guide before completing this form as it includes essential information in support of the evidence required. If you are unsure of the criteria requirements or need further information, then please check with your local county association or contact NALC at LocalCouncilAwardScheme@nalc.gov.uk

Completed sections required for each award level:

- If you are applying for Bronze level complete the Bronze criteria section
- If you are applying for Silver complete the Bronze and Silver criteria sections
- If you are applying for Gold complete the Bronze, Silver and Gold criteria sections

The exception to the above is if you have achieved an award within the last 12 months, then the section for that level award (and the preceding one) need not be completed.

All relevant sections of the form must be completed with evidence provided for the level that you are applying for. Otherwise, this could result in a delay to your application.

Application Tips

- Check all relevant documents are attached with your submission and hyperlinks provided are working correctly.
- Hyperlinks to the council's website must be to the exact evidence required. If this is not possible then include details of how the evidence can be found (i.e. menu, sub-menu etc).
- All published policies and documents must be tailored/personalised to the council.
- Check policies and procedures are not overdue for review. It is best practice to include a review date on all relevant documents and for Silver/Gold award levels the next review date must be included.
- If you are providing minutes as evidence, it is important you include the specific minute reference.
- For the Silver and Gold award levels, a more in-depth assessment will be undertaken of the evidence provided for the preceding award levels. For Gold in particular, the assessment panel will be looking for evidence of best practise throughout the application.
- A column has been provided on this form for any supporting comments you may have.

LOCAL COUNCIL AWARD SCHEME BRONZE

BRONZE RESOLUTION

Please provide hyperlink to minutes: Meetings & Minutes - Drayton Bassett Parish Council

The Council must confirm by resolution that all documentation and information is in place for the Bronze award (See Guide for wording)

Please provide a direct hyperlink for evidence that is published on the council's website. For all other evidence please specify attachment provided.

Criteria	Hyperlink or Attachment	Supporting Comments (if any)
1. Standing Orders	Standing Orders Approved May 2025.pdf	
2. Financial Regulations	Financial Regulations May 2025 - Approved.pdf	
3. Code of Conduct and a link to councillors' registers of interests	Reformatted September 2024.pdf	Register of Interests: Your Councillors - Drayton Bassett Parish Council
4. Accessibility statement	Accessibility Statement - Drayton Bassett Parish Council	
5. Publication scheme	DBPC Publication Scheme Nov 2024.pdf	
6. Complaints procedure	Complaints policy V2 Final Nov 2023.pdf	
7. Privacy notice	Privacy policy.pdf	
8. Last annual return	https://www.draytonbassett-pc.gov.uk/Financial_Reports.aspx	

9. Transparent information about council payments	Meetings & Minutes - Drayton Bassett Parish Council	All financial transactions are at the end of the minutes and bank reconciliations are posted as an attached file to the agendas
10. Calendar of all meetings including the next annual meeting of electors	Parish Council - Drayton Bassett Parish Council	Also shown here: Meetings & Minutes - Drayton Bassett Parish Council
11. Minutes for at least one year of full council meetings and (if relevant) all committee/sub-committee meetings	Meetings & Minutes - Drayton Bassett Parish Council	
12. Current agendas	Meetings & Minutes - Drayton Bassett Parish Council	
13. The Budget and Precept information for the current or next financial year	https://www.draytonbassett-pc.gov.uk/Financial_Reports.aspx	https://www.draytonbassett-pc.gov.uk/Financial_Reports.aspx
14. Biodiversity policy	https://www.draytonbassett-pc.gov.uk/Policy_Documents_25403.aspx	
15. Council contact details and councillor information in line with the Transparency Code	Parish Council - Drayton Bassett Parish Council	Your Councillors - Drayton Bassett Parish Council
16. Action plan for the current year	Version 1 June 2023.pdf	Plus projects detailed in the budget.
17. Evidence of consulting the community	News - Drayton Bassett Parish Council	(1) Facebook Also consult through door to door survey evidence at minute 60: 175716-Signed_Minutes_redacted.pdf Door to door survey undertaken for the installation of Speed Awareness Signs – in minutes of September meeting
18. Publicity advertising council activities	News -	(1) Facebook

	Drayton Bassett Parish Council	
19. Evidence of participating in town and country planning	Planning Applications - Drayton Bassett Parish Council	Comments on planning applications are recorded in minutes too eg July 2025 (Minute 57): 190719-03_July_2025_Minutes_Draft.pdf September 2025 (minute 86) https://www.draytonbassett-pc.gov.uk/_UserFiles/Files/_Minutes/190720-Draft_Minutes_Sept_2025.pdf
20. Evidence of publicising elections and vacancies on the council	New Parish Councillor sought! - Drayton Bassett Parish Council	Posters also on notice boards.
21. Risk management policy	Risk Register May 2025 - Approved.pdf	
22. Register of assets	Asset Register 2024 - 2025 for website.pdf	
23. Up-to-date insurance policies that mitigate risks to public money	policy_schedule.pdf	
24. Evidence of considering the impact of the council's functions and decisions on crime and disorder in local area		Standing item in the minutes for the local police to attend and feedback on crime issues
25. Disciplinary and Grievance procedures	DBPC Grievance Procedure for employeesv May 2022.pdf	
26. A policy for training and development of staff and councillors	Microsoft Word - Traiing Policy September 2025 DRAFT	
27. A record of all training undertaken by staff and councillors in the last year		Councillors – Chairman - Training Course - Planning Making Effective Representations October 2025 Chairman - Training Course - Explore Chairmanship June 2025 Full Councillor Induction Session following mass co-option – November 2024

		Clerk See attached PDF's
28. A current clerk who has achieved 12 CPD points in the last year	Yes	See attached PDF's
29. Signed up to the Civility & Respect Pledge and a Dignity at Work policy	Yes	September 2025